Implement IAM User Roles and Policies (Week 4)

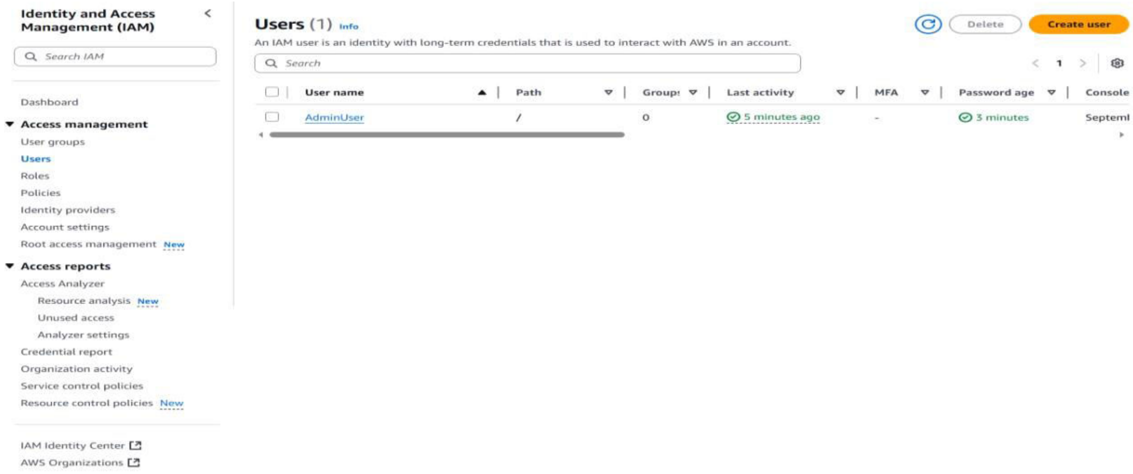
Internship at SkillifyZone

By: Muhammad Qamaruddin

Use Cases of IAM Roles & Policies

- **Separation of Duties –** Different teams (Admins, Developers) get only the permissions they need.
- **Security –** Reduces risk by applying the principle of least privilege.
- **Compliance –** Helps meet organizational and regulatory security requirements.
- **Scalability –** Easy to manage permissions as the number of users and resources grows.

SS of IAM dashboard

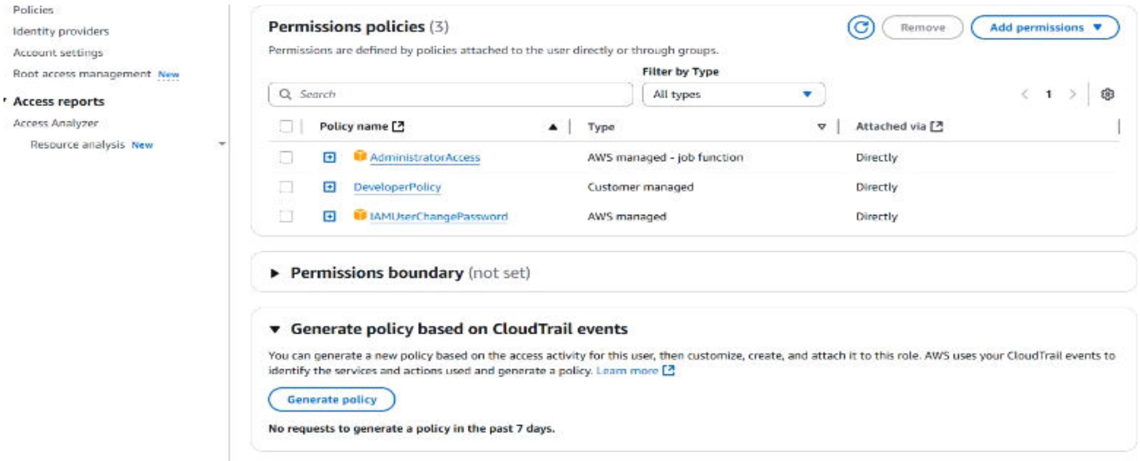


Users (1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Path	Group:	Last activity	MFA	Password age	Console
□	AdminUser	/	0	5 minutes ago	-	3 minutes	Septeml

<u>SS of Created Policies</u>



Permissions policies (3)

Permissions are defined by policies attached to the user directly or through groups.

□	Policy name	Type	Attached via
□	AdministratorAccess	AWS managed - job function	Directly
□	DeveloperPolicy	Customer managed	Directly
□	IAMUserChangePassword	AWS managed	Directly

▶ **Permissions boundary** (not set)

▼ **Generate policy based on CloudTrail events**

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

No requests to generate a policy in the past 7 days.